

UNITED STATES DISTRICT COURT

SOUTHERN

DISTRICT OF

UNITED STATES COURTS
SOUTHERN DISTRICT OF TEXAS
FILED
APR 23 2010
Dwight S. Bradley, Clerk of Court

UNITED STATES OF AMERICA
V.

CRIMINAL COMPLAINT

THOR ALEXANDER MORRIS

Case Number: H-10-352M
W

(Name and Address of Defendant)

I, the undersigned complainant, state that the following is true and correct to the best of my

(Date)

the Southern District of Texas defendant(s) did,

(Track Statutory Language of Offense)

knowingly and with the intent to defraud attempt to access a protected automated teller machine, without authorization and by means of such conduct further intended to fraud and attempt to obtain money from the said protected access device.

in violation of Title 18 United States Code, Section(s) 1030(a)(4) and (b).

I further state that I am a(n) FBI and that this complaint is based on the
Official Title
facts related in the affidavit attached hereto and made a part of this complaint.



Signature of Complainant

Karen Ann Marinos

Printed Name of Complainant

Sworn to before me and signed in my presence,

April 22, 2010

Date

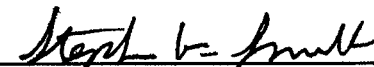
at

Houston, Texas

City and State

Magistrate Judge Stephen Smith

Name and Title of Judicial Officer



Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Karen Ann Marinos (Affiant), being duly sworn, depose and state:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI). I have been a Special Agent since May 19, 2002. I am currently assigned to investigations involving cyber crimes, crimes involving computer intrusions, Internet crimes against children, online child exploitation, as well as other violent crime investigations. Since 2002, I have investigated approximately ninety (90) cyber crime or computer criminal matters. I have participated in the execution of over one hundred forty (140) search warrants and seized evidence of such violations. I have participated in over twenty (20) arrests of people who commit cyber crime violations and I have interviewed over fifty (50) subjects and greater number of victims or witnesses. I have formally charged over fifteen (15) subjects. Excluding Grand Juries, I have testified on more than five (5) occasions during hearings and trials. I have received extensive training in the investigation of computers, telecommunications, and other technology crimes. In addition, I have gained experience in interviewing and interrogation techniques, child forensic interviews, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence identification, computer evidence seizure, and computer evidence processing. I have attended training classes and seminars concerning computer crime, those traveling over state lines to commit computer crimes, and the sexual exploitation of children on the Internet. I have had the opportunity to investigate numerous examples of individuals who commit violations of Title 18 U.S.C. § 1030(a)(4). Title 18 U.S.C. § 1030(a)(2) and Title 18 U.S.C. § 1030(a)(4), is defined as follows:

2. This Affidavit is made in support of a criminal complaint charging Thor Alexander Morris with violating 18 U.S.C. § 1030(a)(4)and(b) which makes it a crime to knowingly and with intent to defraud, attempt access a protected computer without authorization and by means of such conduct furthers the intended fraud and obtains anything of value. I am familiar with the information contained in this Affidavit based upon the investigation I have personally conducted and my conversations with other law enforcement officers involved in this investigation, or who have engaged in numerous investigations involving computer crimes, fraud and related activity in connection with computers.

DEFINITIONS

3. An Automatic Teller Machine, also known as Automated Teller Machine, (ATM) by definition is a computerized telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for the cashier, human clerk or bank teller. On most modern ATM's the customer is identified by inserting a plastic card with a magnetic stripe or a chip and pushes the proper coded buttons. ATM's were first developed in modern form in 1968.
4. A Walmart pre-paid Green Dot card is a VISA or MasterCard that is purchased at Walmart stores, a product result of Walmart partnering with Green Dot Corporation. The PrePaid VISA card does not check one's credit score and Walmart does not require one to have a bank account to own one. An individual can charge a Walmart PrePaid card by using a Green Dot MoneyPak, direct deposit into the PrePaid card amount or cashing a check and the check amount is reflected in the PrePaid card balance. The Walmart

PrePaid card can be used anywhere where VISA or MasterCard is accepted, including ATM's.

5. Instant messages are a form of real-time direct text-based communication, also known as online chats, between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet. Instant Messenger programs, such as Yahoo! Messenger often have buddy lists or contact lists. It is known within the Instant Messenger community that individuals who have Yahoo e-mail addresses such as johndoe@yahoo.com that the prefix of the e-mail address "johndoe" can also be used as the individual's Yahoo! Screenname.

DETAILS OF INVESTIGATION

6. On March 22, 2010, Brian Rhett Martin reported the following to Special Agent Karen Ann Marinos and Special Agent Noel C. Due:
7. Morris approached Brian Martin to conduct some illegal activities related to hacking into ATM machines. Brian Martin told Morris that he was not interested in conducting any illegal activities because he just got out of prison and did not ever want to go back. The fact that Brian Martin was a convicted felon excited Morris and resulted in him confiding in Brian Martin. Through several additional communications, Morris approached Brian Martin to identify and provide locations of Tranax Mini-Bank 1500, 1700, and 2000 ATM machines. Specifically Morris requested that Brian Martin place a GPS tracking device on an ATM maintenance man's vehicle so that Brian Martin may identify many locations of the specific types of ATM's. Morris then planned on flying to Houston, meeting Brian Martin, and traveling to each ATM machine. Morris informed Brian Martin that he had a way to insert a specific password to gain unauthorized access to the

ATM machines. Morris planned to change the denominations electronically within the ATM software to make the ATM think that it contained cartridges of one dollar bills instead of the actual bills, worth twenty dollars each. Then Morris would specifically purchase Walmart "Green Dot" PrePaid cards worth \$400.00 each with a false identification. While at each ATM, Morris would insert a Walmart Green Dot card, ask the ATM to withdraw \$400 in one dollar denominations but actually receive \$8,000 (400 x \$20). Morris planned on withdrawing about \$8,000 to \$10,000 per ATM, only utilizing one to two Walmart Green Dot cards. Morris promised Brian Martin that he would provide 50% of his profits to Brian Martin for his assistance in locating the ATM machines and accompanying him throughout his criminal activities in Houston.

8. To prove to Brian Martin that Morris knew what he was actually in a position to gain unauthorized access into the specific Tranax ATM machines, Morris sent Brian Martin a manual titled Tranax_MB_Operator_Manual that describe the key sequence to enter the specific ATM machine's programming and then the master password. Morris also sent Brian Martin two other manuals on how to gain unauthorized access into another type of ATM machine and a manual for a supermarket/store point of sale credit/debit card processor.
9. Through their many communications, Brian Martin and Morris shared Facebook profiles and became each other's Facebook friends. Brian Martin established that Morris's Facebook profile was named "Thor Morris". Brian Martin also discovered that Morris works at some sort of chain grocery store or department store as a "Front Line Manager." Morris informed Brian Martin that he has the capability to void true customer transactions, such as grocery transactions, then utilize the voided money to install that

money onto PrePaid Visa cards or money orders. The books for the store will always be even and he is his own manager therefore no other person is in the position to audit or verify Morris's work. Morris also informed Brian Martin that he has learned how to hack into his store's Western Union machine and could wire money to anyone without record.

10. Morris and Brian Martin talked about the time frame that Morris would come to town.

Morris planned to travel to Houston the first or second week of April 2010. Morris confided that he has conducted similar ATM hacking trips in Tennessee, Florida, South Carolina, and Virginia. Morris and Brian Martin planned to monitor Houston Police traffic with a radio that Morris purchased from Brian Martin, while they were going to each location of the ATM's in the Houston area. Brian Martin informed Morris that he had approximately 32 ATM machines mapped out for Morris's trip. Brian Martin decided to report the matter to the FBI. Brian Martin gained as much information about Morris, including pictures of Morris, to provide to the FBI for further investigation. Brian Martin planned on introducing the FBI to Morris, the FBI being his buddy "Leo." Brian Martin conducted all these actions on his own accord and before he reported the matter to the FBI.

11. During the initial interview Brian Martin provided Affiant a CD containing the three referenced manuals above, several Facebook pictures of Morris, and three captured Yahoo! Messenger chat logs. The following are relevant excerpts of the captured instant messages provided by Brian Martin:

12. Instant Message #1 on March 18, 2010:

a. File Name: im-3-18-10.txt

- b. Summary: Brian Martin and Morris were planning a date to hack into ATM machines located in Houston. Brian Martin provided GPS coordinates and maps of several ATM machines. Morris informed Brian Martin that he was about to hack into ATM machines in the Raleigh area. Morris explained that he hacked into several ATM's in Tennessee, Florida, where Morris resided (Jacksonville, NC), South Carolina, and Virginia. Morris explained that he had a disguise to hide his face.

13. Instant Message #3 on March 21, 2010:

- a. File Name: im-3-21-10.txt
- b. Summary: Morris discusses the Triton 8100 ATM machines are easy to hack into, discussed the differences between the Tranax ATM, and the lack of remote log or verification. Brian Martin informed Morris that they have 31 target ATM machines in Houston. Both discuss the financial potential probably reaching \$248,000 when they commit the ATM intrusions. Morris joked that 31 ATM machines would be 31 counts of "grand ATM theft," how their crimes would at least be a felony, and the fact that they would have to be breaking a few laws. Morris discussed how he discovered how he got into ATM hacking and how he researched how to do it.

14. On March 31, 2010, Brian Martin provided the FBI consent to search his personal e-mail account hortonandgregory@att.com and consent to assume his online identity fitnaberich@yahoo.com and Yahoo! Messenger Screenname "fitnaberich" in order to pursue Morris for his planned criminal activities. Affiant and SA Noel C. Due are certified as Cyber Online Undercover Agents. Affiant has also been certified as an

Innocent Images Undercover Agent and participated in Phoenix and Houston online undercover investigations since March 2006. Your Affiant has experience in communicating with criminals in online capacities, some of which include people who intend to travel with the purpose of committing federal crimes. Your Affiant and SA Noel C. Due conducted the following undercover sessions:

15. In March 2010, Affiant conducted several records checks on Thor Alexander Morris. Your Affiant was able to retrieve a driver's license photograph of Morris from North Carolina. The driver's license photograph matched the pictures that Morris sent for his fake driver's license identification as well as his pictures posted on his Facebook account online.
16. On April 19, 2010, Affiant verified through FBI airport Liaisons that Morris's flight itinerary is valid and purchased by Thor Alexander Morris, 555 Chief Court, Jacksonville, NC.
17. On April 22, 2010, Morris traveled from Jacksonville, North Carolina to Atlanta, Georgia via Delta Flight #5491 and then traveled from Atlanta, Georgia to Houston, Texas IAH via Delta Airlines flight DL Flight #4356. This information was reported to Affiant by FBI Airport Liaison Andrew Phimpavong. Special Agent Robert Guerra reported to your Affiant that he observed that Morris picked up a checked bag, a blue Nautica suitcase, and telephonically contacted SA Noel C. Due, who was acting in an undercover capacity as Leo. Morris met SA Noel C. Due who picked Morris up from IAH Terminal A Arrivals. Morris wore jeans, a gray t-shirt, a striped button down shirt, and a tan baseball hat.

18. On April 22, 2010, at 7:30 am, Affiant met the General Manager of Mercado 6, 7355 Hwy 6 South, Houston, TX 77083, and the owner of the ATM machine located within Mercado 6. The General Manager and the ATM owner provided the FBI consent and access to utilize the building and the ATM for the planned criminal activity. The owner of the ATM verified that the ATM was functioning properly. Affiant was present at the Mercado 6 for the entire operation and ensured that no other person utilized the ATM machine.
19. On April 22, 2010, several members of the FBI Houston Area Cyber Crimes Task Force conducted surveillance and reported the following activities to Affiant: Morris and SA Noel C. Due travelled from IAH to Walmart, 3506 Highway 6 South, Houston, Texas. Morris changed his shoes, jeans, shirt, and hat to a white pair of pointed dress shoes, another pair of jeans, a white button down shirt, and a black baseball cap. SA Noel C. Due and Morris then entered Walmart where Morris made a purchase. SA Noel C. Due and Morris left Walmart and drove around to several streets and shopping centers in the immediate area. SA Noel C. Due then drove to Mercado 6. After arriving at Mercado 6, Morris donned a long black curly hair wig and walked into Mercado 6 with SA Noel C. Due.
20. On April 22, 2010, Affiant was one of many members of FBI Houston Area Cyber Crimes Task Force who conducted surveillance on SA Noel C. Due and Morris entering Mercado 6. At approximately 11:30 am, Affiant and other members of the FBI Houston Area Cyber Crime Task Force placed Morris under arrest in violation of 18 U.S.C. § 1030(a)(4) for attempting to gain unauthorized access into an ATM machine.

21. On April 22, 2010, SA Noel C. Due informed Affiant of the following observations regarding Morris. Morris brought one travel bag containing clothes, a laptop computer, a phone, a black curly hair wig, a fake mustache, and a large amount of twenty dollar bills. SA Noel C. Due picked up Morris at the airport. Morris was wearing a gray t-shirt, blue jeans, a button down shirt, and tan baseball cap. Morris stated that he did not bring any PrePaid debit cards that could be used to withdraw money upon arrival of the targeted ATM's. However, Morris brought cash and planned to go to a Walmart to put money on a card prior to travelling to the first ATM. Morris requested that SA Noel C. Due take him to a Walmart to purchase the PrePaid cards. In the Walmart parking lot, Morris changed clothes, putting on a white button down shirt with design pattern, another pair of blue jeans, white shoes he said "Rick James" would wear, and black baseball cap. He also revealed a black hair wig he called his "Rick James" wig that he had used in the past when he compromised other ATM's. Morris and SA Noel C. Due went into the Walmart where Morris purchased a Walmart Green Dot PrePaid debit card for \$3 and charged the card with \$410 for use. Morris explained that the purpose of this was to have \$400 to "withdraw" and money left over for the ATM fees.

22. On April 22, 2010, SA Noel C. Due informed Affiant that following the Walmart Green Dot PrePaid debit card purchase, Morris explained that he needed to register and activate this card online. In order to do this, Morris and SA Noel C. Due returned to their vehicle where Morris utilized his laptop computer and attempted to connect to any unsecured wireless connection he could find. To accomplish this, Morris made attempts to identify open wireless access points at several businesses in the area to include, Walmart, McDonalds, Pizza Hut, International House of Pancakes, several mini markets, and strip

malls, before obtaining an unsecured wireless Internet connection outside El Rio del Sol apartment complex at the intersection of Rio Bonito and Tres Lagunas, Houston, TX, near Highway 6. When Morris obtained the wireless Internet connection, Morris accessed walmartmoneycard.com a location on the Internet where a customer usually registers their name, address, phone number, and establishes a pin for debit withdraw. Morris entered the information Barack Obama, and entered a fictitious address and phone number. Morris registered the pin as "1234." Morris explained the card was registered and that they were ready to travel to the ATM. During the travel, Morris explained that he did not have gloves with him but he planned to wipe down the machines and "be careful not to touch the sides." Morris intended to gain unauthorized access to 35 ATM machines, which he requested Leo to identify, and take between \$250,000 and \$350,000 throughout the day. Morris asked if SA Noel C. Due received the package that he shipped to Leo a few days prior. SA Noel C. Due explained that the package never arrived. Morris produced a receipt for USPS mail package sent April 16. Morris disclosed that the contents of the package contained an altered suit jacket with the pocket deepened to conceal large amounts of money and other "tools." Morris also discussed he worked at Food Lion in Jacksonville, North Carolina, that he had a friend who also worked at Food Lion that assisted him in hacking into computer systems and stealing credit card information, he said he has compromised several ATM's on the east coast, and the Navy Federal Credit Union and Walmart are two of his targets. Morris also disclosed that he was a "hacker" and that he conducted many other criminal activities involving computers and fraud. Morris also discussed eluding the law, legal process, and law enforcement, namely the "FBI."

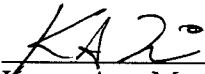
23. On April 22, 2010, SA Noel C. Due informed Affiant that upon arrival at Mercado 6, Morris walked up to the ATM, he pressed the "ENTER" "CLEAR" "CANCEL" "1" "2" "3" which resulted in Morris accessing the "Enter Password" screen. Morris made at least three attempts to enter the default password of "555555" to gain unauthorized administrator access, or complete access to all ATM functions. Morris also attempted to gain unauthorized access by entering "111111." Subsequently, the FBI interrupted Morris and arrested him without incident.
24. On April 22, 2010, Affiant and SA Deborah Gannaway interviewed Thor Alexander Morris at the Houston FBI Office, 1 Justice Park Drive, Houston, TX. Morris was administered his Miranda rights and waived his rights at the beginning of the interview. Morris stated during the arrest interview that "Brian and Leo set it all up" and Morris travelled to Houston "to help them out." Morris explained that he met Brian Martin online through centurionreplica.com because Brian Martin wanted to buy several American Express Black Cards. Morris was impressed by Brian Martin's criminal history and they quickly became online friends. Morris utilized his cell phone 910-548-6665, thor.moris@gmail.com, alexander90.morris@gmail.com, and/or Yahoo! Screenname "rsdbaby" to communicate with Brian Martin. Morris and Martin became Facebook friends. Morris told Brian Martin that he has hacked into Tranax ATM machines in the past, in other states, and he was able change the denominations from \$20 bills to \$1 bills then withdraw the money with PrePaid cards. Morris informed Your Affiant that he fabricated the story from an old youtube.com video. Affiant asked Morris to describe the steps that he would use to gain unauthorized access at the ATM that he planned to compromise that day. Morris explained that he would enter the keys "Enter" "Clear"

“Cancel” “1” “2” “3” which would result in the enter password screen. Morris then planned to enter “55555” which would give him access to the “Operator Menu.” Morris then planned to navigate to the “currency denomination” page where he planned to change the denominations from \$20 bills to \$1 bills. Morris planned to hit the “cancel” button “a few times” which would result in the default customer screen. Morris planned to enter a Walmart PrePaid Green Dot card and withdraw money from the ATM. Morris said that he utilized the Walmart PrePaid Green Dot cards because you can remain anonymous and untraceable. SA Deborah Gannaway placed the Walmart Green Dot PrePaid card that was removed from Morris’ pocket during the arrest on the desk in front of Morris. Morris admitted that was the Walmart Green Dot PrePaid card that he purchased to defraud the ATM that day after he altered the settings.

25. During the interview of Morris, Morris disclosed to Affiant that he and Brian Martin planned to find several target ATM’s to conduct this criminal activity. Morris understood that Brian Martin and his friend Leo found and mapped 33 ATM’s that they would target. Morris explained that Brian Martin became angry at him for not paying him on time for a surveillance radio he agreed to pay for. Brian Martin told Morris that he did not want to be involved any longer but if Morris was still interested then he could contact his friend Leo. Morris initiated contact with Leo and explained they had several communications, over e-mail and one phone conversation, regarding Morris travelling to Houston to meet Leo and compromise ATM’s. Morris planned on travelling to Houston on Thursday, April 15, 2010 but did not have enough time to prepare but both rescheduled for Morris to travel on Thursday, April 22, 2010.

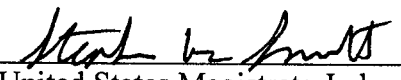
26. During the interview of Morris, Morris disclosed to Affiant that he met Leo on the morning of April 22, 2010 and after speaking with Leo he understood that they were going to target 35 ATM's. Morris understood that they would potentially profit \$350,000. Morris also said that he didn't know if the ATM's would actually contain upwards to \$10,000 each. Morris explained that he and Leo travelled to Walmart the same morning for Morris to purchase a Walmart Green Dot PrePaid card. Morris purchased one Walmart Green Dot PrePaid card for \$410 plus a \$3 charge for the card. Morris disclosed that he had to activate the Walmart Green Dot PrePaid card therefore he and Leo drove around to find an unsecured wireless connection. Once obtaining an unsecured wireless connection, Morris connected to the Internet to activate the Walmart Green Dot PrePaid card. Morris registered the Walmart Green Dot PrePaid card under Barack Obama, with the White House address, 1600 Pennsylvania Avenue, Washington D.C., and made up a fake driver's license number. Morris admitted that he utilized a netbook laptop, labeled "EEE," to access the Internet in Houston. Morris explicitly purchased the laptop for his illegal activities in Houston only two days prior to his travel. Morris explained that he has never really performed the unauthorized access on ATM's in the past but only made up the elaborate story to tell Brian Martin and Leo. Morris admitted that he purchased the plane ticket, travelled to Houston, made several preparations, purchased the Walmart Green Dot PrePaid card, and made actions towards gaining unauthorized access to 35 ATM's. Morris planned to split half of all earnings from the compromised ATM's with Leo. Morris believed that leaving Houston with \$40,000 would have been more realistic because some of the ATM's may have been patched. At this point of the interview, Morris asked for an attorney.

27. On April 22, 2010, Affiant and SA Noel C. Due performed an inventory on Morris' travel belongings and items removed from Morris prior to his transportation to the Houston Police Department's Central Jail. The following items inventoried were pertinent to Morris' criminal activities: Black curly hair wig, one Walmart Green Dot PrePaid debit card, two Delta boarding passes, two cell phones, one black hat, one pair of jeans, one North Carolina driver's license bearing the name Thor Alexander Morris, one goatee beard kit, one bottle Cinema Secrets adhesive remover, one bottle Cinema Spirit gum adhesive, gray t-shirt, one button down striped long sleeve shirt, one Walmart receipt for PrePaid card, one Walmart Green Dot Money Card packaging with Walmart bag, one business card Violet's Alterations in Jacksonville, North Carolina, one U.S. Postal Service Delivery Confirmation receipt, one USB thumb drive, one blue Nautica travel bag containing clothes and other personal items, and one Asus laptop computer.
28. Based upon the information delineated above, Affiant believes that probable cause exists for the issuance of a Criminal Complaint charging Thor Alexander Morris with a violation of 18 U.S.C. § 1030(a)(4) and (b) which make it a crime to knowingly and with intent to defraud, attempt to gain access a protected computer without authorization and by means of such conduct furthers the intended fraud and obtains anything of value.



Karen Ann Marinos
Special Agent, FBI

Subscribed and sworn before me this 23rd of April, 2010, and I find probable cause.



United States Magistrate Judge